

REMARKS

Claims 1-27 are pending in the Application.

Claims 1-27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Ogawa et al.* (U.S. Patent No. 6,754,736), herein referred to as *Ogawa*, in view of *Willman, B. M.* (U.S. Patent No. 5,418,956), herein referred to as *Willman*.

I. EXAMINER'S RESPONSE TO ARGUMENTS

In an attempt to obtain clarification of the Examiner's response, Applicant's representative held a phone conference with the Examiner on 11/15/2005. During this informal interview, Examiner was unable to provide any further details to the argument against independent claims 1, 10, and 19 than what was already stated in the final rejection. *See* Office Action from 10/25/2005, p. 2, lines 11-14. On 11/17/2005, Applicant's representative held a phone interview with the Examiner's Supervisor and obtained the suggestion from the Supervisor to respond with appropriate arguments. On 11/22/2005, Applicant's representative received a voicemail from the Supervisor, that the merits of the case could be considered for determining the different viewpoints on the art in the claim. On 12/12/2005, the Supervisor was contacted and the issues regarding the Examiner's response and the interpretation of the prior art were discussed. On the same day, the Supervisor contacted Applicant's representative and suggested that the prior art did not necessarily support the Examiner's reasoning and that a withdrawal of the final rejection could be argued.

The Examiner states regarding claims 1, 10, and 19 in the Response to Arguments that

...Ogawa teaches that requests are analyzed and are not serviced if they do not match the request list (see Fig. 5 and Fig. 9). The request list is a list of authenticated users, so by analyzing the source of request Ogawa determines if the request is from an unauthenticated user. *See* Office Action from 10/25/2005, p. 2, lines 11-14.

Applicant respectfully traverses the Examiner's interpretation of the reference. *Ogawa* does not teach "that requests are analyzed and not serviced if they do not match the request list." The user requests in *Ogawa* are always accepted for addition into the request list. Figures 5A and 5B in *Ogawa* (and related Figure 4) describe a process for adding a new list element to the request list. *Ogawa*, col. 6, lines 6-12. Figure 9 in *Ogawa* describes a process performed by a data processing device, illustrated in Figure 2, in response to an input/output request from a user process. *Ogawa*, col. 9, lines 15-21, 63-65. There is no language or figure in *Ogawa* that teaches "...determining if the request was transmitted from a user space or a kernel space..." and no language that teaches "...determining if said request from said unauthenticated user [from user space] fails to satisfy a security requirement..." as in claims 1, 10, and 19. In fact, neither *Ogawa* nor *Willman*, singly or in combination, meet these two distinct and successive claim limitations. The cited references (Fig. 5 and Fig. 9) do not support the Examiner's statement quoted above. Neither was the Examiner able to provide any further explanation in affirmation of these statements upon phone inquiry. Neither did a further inquiry by the Supervisor affirm the above cited statement.

Further regarding claim 19, the Examiner states that "one...would have equated not servicing the request with the denial of the request." See Office Action from 10/25/2005, p. 2, lines 16-17. Applicant asserts that there is no language in *Ogawa* that refers to not servicing requests from user space. Thus the Examiner's response is without support from *Ogawa*.

The Examiner further responds that "...broad but reasonable interpretation of the claims is applied, while the limitations from the specification, that Applicant is relying on, are not read into the claims." See Office Action from 10/25/2005, p. 2, line 22 to p. 3, line 1, emphasis added. The Examiner does not indicate which limitations are being referred to here, and was unable to provide clarification of this statement upon phone inquiry. Applicant respectfully traverses and asserts that arguments in support of the claim language over the prior art, not for limitations from the specification, have been presented.

The Examiner further recites *Willman*, abstract and Figure 7, as providing motivation for modifying *Ogawa* with *Willman*. See Office Action from 10/25/2005, p. 3, lines 6-7. Applicant respectfully traverses and asserts that no effective rebuttal of Applicant's previous arguments has been presented. The cited content in *Willman* does not provide any motivation to combine. Thus in contrast to the Examiner's response, neither *Ogawa*, nor *Willman*, taken singly or in combination, renders claims 1-27 obvious.

Additionally, the Examiner claims that the specification recites the term "user kernel." See Office Action from 10/25/2005, p. 3, lines 8-10. Applicant respectfully traverses and asserts that a search of the present specification, as published document no. US 2003-0037252 A1, did not reveal any instance of the term "user kernel." The Examiner has not provided any reference where said term is found in the specification. Thus, the Examiner's response does not appear to be accurate.

As a result of the foregoing, Applicant respectfully requests that the final rejection be reconsidered, and asserts, in view of the arguments presented in support of claims 1-27, that the rejection of these claims be withdrawn.

II. REJECTIONS UNDER 35 U.S.C. § 103(a)

Claims 1-27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Ogawa* in view of *Willman*. In response, Applicant respectfully traverses these rejections.

As to claims 1, 10, and 19, the Examiner recites regarding *Ogawa* that:

Ogawa shows that a request is sent from [sic] the user space (40) to kernel (50) – see Fig. 2. The limitation "determining if the request was transmitted from a user space...of the computer system" is met by request acceptance process depicted in Figs. 5A and 5B. See Office Action from 10/25/2005, p. 4, lines 15-18.

Applicant respectfully traverses. *Ogawa* does not teach essential limitations of claims 1, 10, and 19, in particular the step of "...determining if said request was transmitted from a user space or a kernel space of a memory space of said computer system,

wherein if said request was transmitted from said user space then said user is an unauthenticated user...." In fact, the Examiner has completely failed to address the underlined language. For this reason alone, the Examiner has failed to prove a *prima facie* case of obviousness. *Ogawa* does not teach processing requests from unauthenticated users or any processes for authenticating users. Fig. 5A in *Ogawa* illustrates the process in user space adding a new element to the request list for the case of an empty request list. Fig. 5B in *Ogawa* illustrates the process in user space adding a new element to the request list for the case of a non-empty request list. The process illustrated in Figs. 5A and 5B and the flow chart of Fig. 4 of *Ogawa* do not disclose "determining if said request was transmitted from a user space or a kernel space..." *Ogawa* does not disclose determining if a request was transmitted from user space or kernel space and *Ogawa* does not disclose processing requests originating from kernel space. Instead, *Ogawa* discloses processing input/output requests originating in user space via a request list through the kernel asynchronously, such that the instances of notification from the user process to the kernel process are reduced. *Ogawa* col. 4, line 56 to col. 5, line 7 and Fig. 2; col. 6, line 6 to col. 7, line 5 and Figs. 4-5. Therefore *Ogawa* does not meet the limitations recited in method claim 1, computer program product claim 10, and system claim 19.

As to claim 19, the Examiner states that: "Ogawa teaches that requests are analyzed and are not serviced if they do not match the request list (see Fig. 5 and Fig. 9)." See Office Action from 10/25/2005, p. 4, line 20-21. Applicant respectfully traverses. *Ogawa* does not teach "determining if said request was transmitted from a user space or a kernel space..." as in claim 19. Fig. 9 in *Ogawa* illustrates data processing in a device driver I/O request from a process in user space, in particular dividing this process into a kernel thread and an asynchronous thread, which may be processed separately for efficiency. There is no mention in *Ogawa* of not servicing a request "if said request from said unauthenticated user fails to satisfy said security requirement...." as recited in claim 19. *Ogawa* does not mention the denial of requests. *Ogawa* therefore does not meet the limitations in claim 19.

The Examiner further asserts that: "Ogawa, however does not explicitly teach determining if the request from unauthenticated user fails to satisfy the security requirement." See Office Action from 10/25/2005, p. 3, line 21 to p. 5 line 1. The Examiner further cites *Willman* in combination with *Ogawa*:

Referring to the instant claims Willman discloses a method and system for avoiding selector loads Willman shows kernel Address space and Application (i.e. user) address space. Willman teaches that user requests are not processed if the request of r [sic] the application program comes from [sic] the wrong address space. The application program is allocated the address space from 0 to 2 G bytes. The kernel is allocated the address space from 2 G bytes to 4 G bytes. When a task is started its segment descriptor table contains a code segment entry, a data segment entry, and, optionally, a thread environment block (TEB) entry. The code segment entry defines the user code segment with a segment base address of 0, a segment limit of 4 G bytes, and an attribute of execute. The data segment entry defines the user data segment with a segment base address of 0, a segment limit of 4 G bytes, and an attribute of read/write. The TEB segment, for example, has a segment base address of 128K and a segment limit of 64K bytes and an attribute of read and write. Willman shows the use of security attributes for the user space. See Office Action from 10/25/2005, p. 5, lines 2-17.

Applicant respectfully traverses. *Willman* does not teach determining if the request from an unauthenticated user fails to satisfy a security requirement, as in claims 1, 10, and 19. The security requirement of claims 1, 10, and 19 is described in the Application, p. 16, lines 1-14 and in Fig. 7, and *Willman* does not disclose any security requirements for unauthenticated requests. The Application clearly discloses that a security layer retrieves the security requirements and applies them as policy to unauthenticated users. The security requirement in claims 1, 10, and 19 is for unauthenticated requests, and does not compare with the security attributes for the user space as in *Willman*. The Examiner has cited no more than *Willman* disclosing 32-bit protected mode memory addressing in the Intel 80386 architecture, which is well-known in the art. *Willman* discloses a method for preventing certain memory loading operations, while maintaining the integrity of the system memory addressing, which was a well-known issue to one of ordinary skill in the art for often causing software malfunctions and negatively impacting the reliability of multitasking 32-bit protected mode platforms. Thus the so-called security of *Willman* is nothing more than the internal integrity of the operating system during normal operation, referring

to the prevention of segmentation errors, memory leaks, out-of-bounds errors at the segment limit, and similar issues pertaining to 32-bit protected mode memory addressing. Claims 1, 10, and 19 do not contain language pertinent to servicing application errors and do not recite limitations dependent on a certain memory addressing scheme. There is no language or figure in *Ogawa* that teaches "...determining if the request was transmitted from a user space or a kernel space..." and no language that teaches "...determining if said request from said unauthenticated user [from user space] fails to satisfy a security requirement..." as in claims 1, 10, and 19. In fact, neither *Ogawa* nor *Willman*, singly or in combination, meet these two distinct and successive claim limitations. Thus, *Willman* does not address the limitations in claims 1, 10, and 19 and these claims are patentable over *Willman*. In summary, neither *Ogawa* nor *Willman*, singly or in combination, disclose the essential limitations in claims 1, 10, and 19. Thus, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1, 10, and 19 since the Examiner is relying upon an incorrect, factual predicate in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (CAFC 1998).

Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art. M.P.E.P. §2143.01. The Examiner states that:

One of ordinary skill in the art would have been motivated to modify the information processing apparatus servicing request received from the user kernel by adding the functionality to determine if the request meets the security requirements as taught in *Willman* for generating the exception an [sic] the interrupt of the execution of the user instructions (see *Willman* abstract and Fig. 7). See Office Action from 10/25/2005, p. 5, lines 18-22.

Applicant respectfully traverses. The term "user kernel" as used by the Examiner is indefinite. *Willman* does not teach determining if the request meets the security requirements as in claims 1, 10, and 19, as previously discussed in this paper. The interrupt of the execution of user instructions in the abstract and Fig. 7 of *Willman* is unrelated in the art to not servicing a user request if the request from an

unauthenticated user fails to satisfy a security requirement for unauthenticated users, as in claims 1, 10, and 19. The interrupt routine in *Willman*, Fig. 7, teaches the handling of flat and non-flat tasks for restoring the data segment register with the selector shared by the application and the kernel, in case of application error in a 32-bit protected mode environment. The present application and claims, however, do not pertain to servicing application errors and do not recite limitations dependent on a certain memory addressing scheme. Therefore, there is no suggestion or motivation in *Willman* to combine *Ogawa* with *Willman* to construe the limitations in claims 1, 10, and 19 along the lines of the present invention. Thus, the Examiner has provided no objective evidence which suggests or gives motivation to combine *Ogawa* with *Willman* in construing the rejection. The Examiner's own opinion in support of the combination of references is not objective evidence. There is no prior art reference that provides sufficient motivation or suggestion to combine *Ogawa* with *Willman* at the time of the invention, as combined by the Examiner for rejecting claims 1-27. Claims 1-27 are therefore patentable over *Ogawa* in view of *Willman* and over the prior art. Applicant respectfully asserts that the Examiner withdraw the rejection of claims 1-27 and allow these claims for issue.

Further regarding claims 2, 11, and 20, the Examiner states that, "Willman teaches that request is services [sic] if the requirements are met (see Fig. 6)." See Office Action from 10/25/2005, p. 6, lines 1-2. Applicant respectfully traverses. There is no mention in *Ogawa* or *Willman* of any kind of security requirements that are accessed by the operating system as in claims 1-2, 10-11, and 19-20 and as disclosed in the specification (p. 16, lines 1-14) and in the drawings (Fig. 7) of the Application. In particular, *Willman* does not disclose the case if the user request "does not fail to satisfy said security requirement" and *Willman* does not disclose servicing the request in response to such a determination, as in claims 2, 11, and 20. Instead, *Willman* teaches reporting user faults and kernel faults, which are violations of the 32-bit protected mode memory addressing in the Intel 80386 architecture, during otherwise normal operation of the operating system. In particular, Fig. 6 of

Willman does not show that the request is serviced if the requirements are met as in claims 2, 11, and 20. Fig. 6 of *Willman* shows a flow diagram for an exception handler to restore the data segment register with the selector shared by the application and the kernel, after an interrupt is generated due to application error in a 32-bit protected mode environment. Claims 2, 11, and 20, however, do not contain language pertinent to servicing application errors and do not recite limitations dependent on a certain memory addressing scheme. There is no mention in *Ogawa* or *Willman* of deterring malicious intent from hackers by determining if user service requests from an unauthenticated user do not fail to satisfy security requirements for unauthenticated users, and if so, servicing such requests. In particular, *Willman* does not teach not servicing requests that may otherwise be executable in terms of consistent memory addressing. Thus, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 2, 11, and 20 since the Examiner is relying upon an incorrect, factual predicate in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (CAFC 1998). Claims 2, 11, and 20 are therefore patentable over *Ogawa* in view of *Willman* and over the prior art for at least the reasons presented above in support of these claims and in support of claims 1, 10, and 19. Applicant respectfully asserts that the Examiner withdraw the rejection of claims 2, 11, and 20 and allow these claims for issue.

Further regarding claims 3, 12, and 21, the Examiner provides no support of the rejection of these claims other than the Examiner's own subjective opinion, which is not objective evidence. The Examiner has not even pointed to any language within the prior art for disclosing or suggesting these claims. For this reason, the Examiner has failed to prove a *prima facie* case of obviousness. The cited prior art does not teach or suggest determining if the user service request was transmitted by a manager in kernel memory space configured to establish a secure authorized connection between said user and said kernel space if said user is authorized. Claims 3, 12, and 21 are therefore patentable over *Ogawa* in view of *Willman* and over the prior art for at least the reasons presented above in support of these claims and in support of

claims 1, 10, and 19. Applicant respectfully asserts that the Examiner withdraw the rejection of claims 3, 12, and 21 and allow these claims for issue.

Claims 4-9, 13-18, and 22-27 recite limitations different than in claims 1, 10, and 19. Therefore, the Examiner must specifically address these claims separately from the rejections of claims 1, 10, and 19. The Examiner has failed to prove a *prima facie* case of obviousness in rejecting these claims because the Examiner has failed to specifically address these claim limitations. Applicant respectfully asserts that the Examiner withdraw the rejection of claims 4-9, 13-18, and 22-27 and allow these claims for issue.

III. CONCLUSION

As a result of the foregoing, Applicant respectfully asserts that claims 1-27 in the Application are in condition for allowance, and respectfully requests a withdrawal of the final rejection and allowance of such claims.

Applicants respectfully request that the Examiner call Applicants' attorney at the below listed number if the Examiner believes that such a discussion would be helpful in resolving any remaining problems.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Applicants

By: _____

Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2851